Veera Ohtonen

GDPR:n vaikutukset yrityksen henkilötietojen käsittelyyn

Tradenomi

Liiketalouden koulutus

Kevät 2018

KAJAANIN
AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Tiivistelmä

Tekijä: Ohtonen Veera

Työn nimi: GDPR:n vaikutukset yrityksen henkilötietojen käsittelyyn

Tutkintonimike: Tradenomi (AMK)

Asiasanat: tietosuoja-asetus, GDPR, henkilötietolaki, tietosuoja

Tämä opinnäytetyö käsittelee GDPR:n vaikutuksia yrityksen henkilötietojen käsittelyyn. EU:n yleinen tietosuojalaki astui voimaan 24.5.2016 ja muuttuu pakottavaksi 25.5.2018. Lain soveltaminen on otettu yrityksissä käyttöön jo kahden vuoden siirtymäaikana, vaikkakin ohjeistuksia itse asetuksesta on annettu vielä tämänkin vuoden puolella. Tässä opinnäytetyössä uutta tietosuojalakia tarkasteltiin suuren yrityksen kannalta, mutta sitä voidaan käyttää ohjeena muillekin yrityksille.

Opinnäytetyö tarkastelee tämänhetkistä henkilötietolakia sekä mitä uutta EU:n yleinen tietosuojalaki tuo tullessaan. Opinnäytetyössä pyrittiin kuvaamaan kaikki ne asiat, jotka jokaisella yrityksellä tulisi olla kunnossa uudistuvan tietosuojalain myötä, selkeästi sekä mahdollisimman yksinkertaisesti.

Ensimmäisenä opinnäytetyössä kuvataan tietosuojaperiaatteet. Tämän jälkeen kuvataan rekisterin velvollisuudet rekisterinpitäjänä sekä henkilötietojen käsittelijänä. Opinnäytetyön lopussa esitellään rekisteröidyn oikeudet sekä sopimuksiin liittyviä seikkoja.

Viimeisenä osiona käsitellään yrityksessä tehtyjä konkreettisia muutoksia. Taulukossa on kuvattuna osat, joita yrityksessä tarkasteltiin ja mihin muutoksia jouduttiin tekemään. Suurimmat muutokset yrityksessä kohdistuivat selosteen tekemiseen, kun tulevaisuudessa uusi tietosuojalaki velvoittaa yritykset pitämään yllä selostetta käsittelytoimista.

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Abstract

Author: Ohtonen Veera

Title of the Publication: The effects of the general data protection regulation to company´s personal data protection

Degree Title: Bachelor of Business and Administration

Keywords: The general data protection regulation, GDPR, Personal Data Act, data protection

The thesis deals with the effects the general data protection regulation has on a company´s personal data protection. The regulation was adopted on 14th April 2016 and becomes enforceable on 25th May 2018. The two-year transition period has given time to companies to make the needed changes in their data protection. The point of view in the thesis is that of a big company, but it can be used in other companies as well.

The thesis examines the current personal data acts and what new the general data protection will bring to personal data protection. The purpose in the thesis was to describe all that should be done in companies before the regulation becomes enforceable, as clearly and simply as possible.

The principles of data protection are discussed at the beginning of the thesis. The second part is about the controller´s and processor´s general obligations. After that, the thesis describes the rights of the data subject and what new GDPR will bring to contracts with other controllers and processors.

In the last section the thesis shows what changes were made in the company because of GDPR. The chart shows the parts that were under inspection. The biggest changes were made in the records of processing activities because starting 25th May 2018 the general data protection regulation obligates companies to keep records of all their processing activities.

Sisällys

1 Johdanto

Opinnäytetyössäni tutkin EU:n uutta tietosuojalakia (General Data Protection Regulation, GDPR 2016/679). Työ tehdään erään yrityksen avuksi toteuttaa kaikki tietosuojauudistuksen vaatimat toimenpiteet. Opinnäytetyön toimeksiantaja on Suomessa toimiva suuri matkailun asiakaspalveluun erikoistunut yritys.

Mitä yrityksen tulee huomioida uuden tietosuojalain astuessa lainvoimaiseksi 25.5.2018 ja mitä toimenpiteitä se vaatii yritykseltä? Tutkimusmenetelmä, jota käytän opinnäytetyössäni, on oikeusdogmatiikka eli laintulkinta, tarkoittaen tässä työssä henkilötietolain ja uuden GDPR:n välistä laintulkintaa. Tutkin molempia lakeja rinnakkain ja näiden pohjalta luon mallin, miten yrityksen tulee täyttää uudistuneen tietosuojalain vaatimukset. Lakeina GDPR:n lisäksi käytän muun muassa henkilötietolakia 523/1999 ja lakia yksityisyyden suojasta työelämässä 759/2004.

Ensimmäisenä tulee kartoittaa tietojenkäsittelyn nykytila. Mitä tietoja on ja kenellä ne ovat hallussa? Yrityksen tulee arvioida myös henkilötietojen käsittelyyn liittyvät riskit ja miettiä keinot riskien minimoimiseksi. Uuden tietosuojalain mukaisesti on myös tehtävä selvitys eli rekisteriseloste siitä, millä perusteilla yritys käsittelee hallussa pitämiään henkilötietoja.

Yhtenä merkittävimmistä muutoksista uudessa tietosuojalaissa ovat rekisteröidyn oikeudet. Rekisteröidyn oikeuksiin kuuluu muun muassa unohdetuksi tulemisen oikeus. Tämä tarkoittaa sitä, että yrityksen tulee miettiä, miten se käytännössä varmistaa rekisteröidyn oikeuksien toteutumisen.

Yrityksen tulee arvioida tietoturvaan liittyvät toimenpiteet riskiperusteisesti ja suojata henkilötietojen koko elinkaari. Yrityksen on valmistauduttava ilmoittamaan mahdollisista tietoturvaloukkauksista tietyn ajan kuluessa. Tuleeko yritykseen nimittää tietosuojavastaava?

Lisäksi digitaalisessa muodossa olevien henkilötietojen lisäksi tulee ottaa huomioon kaikki fyysisessä muodossa säilytettävät henkilötiedot. Kuinka niiden säilytystä tulee muuttaa ja kuinka niiden turvallisuus taataan kyseissä yrityksessä?

Uusi tietosuojalaki tuo myös mukanaan kovemmat sanktiot, mikäli yritys rikkoo tai ei noudata asetuksen mukaisia määräyksiä.

2 EU:n tietosuojauudistus ja GDPR

Euroopan Unionin tietosuojalainsäädäntöä aloitettiin uudistamaan vuonna 2012. Silloinen olemassa oleva lainsäädäntö ei enää riittänyt vastaamaan nykyajan tarpeisiin. Uudistuksen myötä haluttiin tehostaa rikollisuuden ja terrorismin turvaa, turvata henkilötietojen suojaa perusoikeutena sekä digitalisaation kehitystä. Tämän uudistuksen myötä syntyi kaksi asiaa: yleinen tietosuojalaki (2016/679) sekä tietosuojadirektiivi (2016/680). Tietosuojadirektiivi koskee esimerkiksi poliiseja sekä muita viranomaisia, jotka käsittelevät henkilötietoja työssään. (Karhula & Kipinoinen 2018; Tietosuojavaltuutetun toimisto 2018.) Tässä opinnäytetyössä keskitytään näistä kahdesta vain GDPR:ään.

EU:n yleinen tietosuojalaki, GDPR (General Data Protection Regulation, 2016/679) tuli voimaan 24.5.2016. Asetuksen antoivat Euroopan parlamentti ja neuvosto. GDPR:n soveltaminen alkaa 25.5.2018. Kahden vuoden siirtymäaika on antanut yrityksille aikaa varautua tulevaan uudistukseen ja varmistaa, että heidän henkilötietojen käsittelynsä ovat lain mukaisia asetuksen astuessa käytäntöön. (Oikeusministeriö 2017.) EU:n uusi tietosuojalaki korvaa vuonna 1995 annetun henkilötietodirektiivin (95/45/EY) sekä muutosta koskevia kohtia henkilötietolaista (523/1999). Yleisen tietosuojalain avulla pyritään luomaan Euroopan Unionille yhtenäinen sekä vahva tietosuojaohjeistus ja näin kehittämään EU:n digitaalisia sisämarkkinoita (Andreasson & Ylipartanen 2015).

Lain tarkoitus on luoda ja varmistaa Euroopan Unionin jäsenmaille laaja, yhtenäinen ja nykyaikainen tietosuojaverkosto. Digitalisaation kehittyessä täytyy tietoturvankin kehittyä. Uudistuksen suurimpia tavoitteita ovat yksilön oikeuksien ja vapauksien vahvistaminen sekä tietosuojan globaalin ulottuvuuden vahvistaminen ja tietosuojalakien noudattamisen valvonnan tehostaminen. (EU:n tietosuoja-asetuksen velvoitteet johdolle 2018.)

Laki tulee koskettamaan kaikkia yrityksiä ja organisaatioita Suomessa sekä muissa EU:n jäsenvaltioissa, jotka pitävät hallussaan henkilötietoja digitaalisessa tai fyysisessä muodossa.

3 Määritelmiä

Henkilötiedolla tarkoitetaan kaikkea sellaista tietoa, josta luonnollinen henkilö (myöhemmin rekisteröity) on suorasti tai epäsuorasti tunnistettavissa (Henkilötietolaki 1:3§). Tällaisia tunnistetietoja ovat esimerkiksi nimi, henkilötunnus, osoite, sähköpostiosoite, puhelinnumero, kuva, pankkitieto tai IP-osoite.

Henkilötietojen käsittelyä ovat kaikenlaiset toiminnot, jotka kohdistuvat henkilötietoihin. Tällaisia toimintoja ovat tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, muokkaaminen, säilyttäminen, käyttö, luovuttaminen, levittäminen, poistaminen ja tuhoaminen (EU yleinen tietosuojalaki artikla 4 kohta 2).

Tietosuoja tarkoittaa yksityisyyden suojaamista henkilötietoja käsiteltäessä.

Henkilötietorekisteri on mitä tahansa yllämainittuja tietoja sisältävä rekisteri. Henkilötietorekisteri voi olla joko atk:n avulla oleva listaus tai vaikkapa manuaalisesti ylläpidettävä mappi, jonne työntekijöiden henkilötiedot on kerätty. (EU yleinen tietosuojalaki artikla 4 kohta 6.)

Rekisterinpitäjä on henkilörekisterin ylläpitäjä. Rekisterinpitäjällä on osoitusvelvollisuus kaikista hallussa pitämistään tiedoista.

Rekisteröity on henkilö, jonka tietoja rekisterinpitäjä käsittelee ja ylläpitää henkilötietorekisterissä.

Henkilötietojen käsittelijä on luonnollinen henkilö, oikeushenkilö tai viranomainen, joka käsittelee yrityksen henkilötietoja rekisterinpitäjän lukuun (EU yleinen tietosuojalaki artikla 2 kohta 8).

Tietosuojavastaava on yrityksen tietosuojan tukipilari. Tietosuojavastaava voi olla yrityksen työntekijä tai ulkoistettu toimija. (Tietosuojavastaavia koskevat ohjeet 2017, 19.)

Tietosuojavaltuutettu on Suomessa toimiva viranomainen, joka valvoo tietosuojalakien noudattamista sekä antaa yrityksille ohjeita lakien soveltamiseen (Tietosuojavaltuutetun toimisto 2013).

Tietoturvaloukkauksella tarkoitetaan vahinkoa, jolloin henkilötietoa tuhoutuu, häviää, muuttuu tai luovutetaan/luetaan luvattomasti. Rekisterinpitäjällä on tietoturvaloukkauksista ilmoitusvelvollisuus. (Talus, Autio, Hänninen, Pihamaa & Kantonen 2017, 32.)

4 Tietosuojaperiaatteet

Henkilötietojen käsittelyssä on noudatettava tietosuojaperiaatteita. Näitä periaatteita ovat käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, tietojen täsmällisyys, tietojen säilytyksen rajoittaminen, tietojen eheys ja luottamuksellisuus ja rekisterinpitäjän osoitusvelvollisuus. (Talus ym. 2017, 12.)

Kuten henkilötietolaissakin on kuvattu, käsittely on lainmukaista silloin kun rekisteröity on antanut suostumuksensa henkilötietojen käsittelyyn. (EU yleinen tietosuojalaki, artikla 6 & artikla 7.) Henkilön aloittaessa työsuhteen ei suostumusta työnantajan asianmukaiseen henkilötietojen käsittelyyn erikseen tarvita.

Tiedot on kerättävä tiettyä, nimenomaista ja lainmukaista tarkoitusta varten eikä niitä myöhemmin saa käyttää eri tavalla, kuin alun perin tietoja kerätessä on ollut tarkoitus. Käsiteltävien henkilötietojen on oltava asianmukaisia ja olennaisia. Tietojen minimointi tarkoittaa, että rekisterinpitäjä saa pitää hallussaan sellaista tietoa, joka on niiden käsittelyn tarkoituksen kannalta olennaista ja tarpeellista (käyttötarkoitussidonnaisuus). (EU yleinen tietosuojalaki, artikla 5 kohta 1.) Tarpeellisuusvaatimus tarkoittaa juuri sitä, että työnantaja saa käsitellä vain työsuhteen luonteen kannalta tarpeellisia tietoja. Tietojen on oltava täsmällisiä sekä aina ajan tasalla. Rekisterinpitäjän on aina varmistettava, ettei se käsittele virheellisiä tietoja. (Henkilötietolaki 9§.) Tarpeellisuusvaatimuksesta ei voida poiketa työntekijän suostumuksella (Laki yksityisyyden suojasta työelämässä 2:3§).

Tietoja on käsiteltävä ainoastaan sen ajan verran, kuin tietojen luonteen mukaan on tarpeen. Esimerkiksi työntekijän työsuhteen päättyessä yrityksellä ei ole enää syytä pitää hallussaan kyseisiä henkilötietoja. Tietoja on käsiteltävä turvallisella tavalla, suojaamalla niitä luvattomalta ja lainvastaiselta käsittelyltä. Tietoja on suojattava myös vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai fyysisiä toimia. (EU yleinen tietosuojalaki artikla 5 kohta 1.)

Rekisterinpitäjällä on osoitusvelvollisuus. Enää ei riitä, että vain noudattaa sääntöjenmukaisuutta, vaan asetuksen astuessa voimaan rekisterinpitäjän on myös kyettävä osoittamaan se. Rekisterinpitäjä on aina vastuussa kyseisten periaatteiden noudattamisesta ja siitä, että tarvittaessa pystyy sen todistamaan, että kyseisiä periaatteita on noudatettu. (EU yleinen tietosuojalaki artikla 5 kohta 2.) Eräs keino osoittaa tämä on toteuttaa edellisten tietojen perusteella laadittava tietotilinpäätös.

Yleisessä tietosuojalaissa on annettu kohta tiedoista, joiden käsittely on kiellettyä ilman rekisteröidyn nimenomaista suostumusta kyseisten tietojen käsittelyyn. Näihin tietoihin lukeutuvat rotu sekä etninen alkuperä, poliittiset mielipiteet, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys. (EU yleinen tietosuojalaki artikla 9 kohta 1.) Erityisten henkilötietojen joukosta terveyttä koskevien tietojen käsittelyä tapahtuu esimerkiksi silloin, kun työntekijä joutuu sairauden vuoksi olemaan töistä pois tai kun sairaus vaikuttaa hänen työntekoonsa.

Tietosuojaperiaatteita tulee noudattaa henkilötietojen käsittelyn kaikissa eri vaiheissa. Tiedon elinkaari muodostuu kolmesta päävaiheesta:

- kerääminen
- säilyttäminen
- tuhoaminen.

Tiedon kerääminen tapahtuu monesti työsuhteen alkaessa tai rekrytointiprosessissa. Yrityksen tulee suunnitella tavoitteet, rajat sekä säilytysajat kerättäville tiedoille: mitä tietoja tarvitaan ja miksi, miten pitkään niitä säilytetään ja miten. (Ahola & Hirvelä 2016.)

Rekisterinpitäjän velvollisuus on pystyä todistamaan toteuttavansa kaikkia yllämainittuja periaatteita tiedon elinkaaren kaikissa vaiheissa. Rekisterinpitäjän velvollisuuksista kerrotaan lisää tämän opinnäytetyön seuraavassa kappaleessa.

Tietosuoja-asetuksen mukaan rekisterinpitäjä ei saa säilyttää tietoja hallussaan yli sen ajan kuin on todella tarpeen. Esimerkiksi työntekijän henkilötietojen käsittelyn oikeellisuus päättyy, kun henkilö lopettaa yrityksessä työskentelyn.

Tämän lisäksi on huomioitava muut lait sekä säädökset samasta aiheesta. Esimerkiksi työsopimuslain mukaan työnantaja on velvoitettu antamaan työtodistus, mikäli sitä pyydetään, kymmenen vuoden aikana työsuhteen päättymisestä (Työsopimuslaki 6:7§). Tämän vuoksi, työntekijän työsuhteen päättyessä, rekisterinpitäjän on hyvä jättää oleelliset tiedot työtodistuksen tekemistä varten säilöön ja hävittää loputkin tiedot kyseisen aikarajan mennessä umpeen.

Rekisterinpitäjällä on velvollisuus tuhota tiedot asianmukaisella tavalla käyttötarkoituksen päättymisen jälkeen. Henkilötiedon elinkaaren loppupuolella tiedon voi hävittää tai anonymisoida. (Hallituksen esitys 9/2018, Yksityiskohtaiset perustelut 2 luku.)

5 Yrityksen velvollisuudet rekisterinpitäjänä

Rekisterinpitäjän tietosuojavelvollisuudet koskettavat kaikkia heidän käsittelemiään henkilötietoja. Näihin kuuluvat yrityksen henkilökunnan, yrityksen asiakkaiden ja yhteistyökumppanien tiedot. Henkilötietojen käsittelyä ovat kaikenlaiset toiminnot, jotka kohdistuvat henkilötietoihin. Tällaisia toimintoja ovat tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, muokkaaminen, säilyttäminen, käyttö, luovuttaminen, levittäminen, poistaminen ja tuhoaminen (EU yleinen tietosuojalaki artikla 4 kohta 2).

5.1 Nykytilan arviointi

Aluksi rekisterinpitäjän on selvitettävä henkilötietojenkäsittelyn nykytilanne. Tulee tarkastaa, miten henkilötietoja tällä hetkellä yrityksessä käsitellään ja vastaavatko ne uuden tietosuoja-asetuksen mukaista käsittelyä. Tärkeää on tutkia, mitä tietoja käsitellään ja ovatko kaikki tiedot tarvittavia. Lisäksi on hyvä tarkastaa missä tietoja fyysisesti säilytetään. Nykytilan arvioinnin jälkeen yrityksen on helpompaa tarkastaa ja lähteä korjaamaan henkilötietojenkäsittelyn prosessit tietosuoja-asetuksen mukaiseksi.

5.2 Tietotilinpäätös

Nykytilan arvioinnin tueksi yrityksen kannattaa laatia tietotilinpäätös (Laadi tietotilinpäätös 2012). Tietotilinpäätös laaditaan tietosuojaperiaatteiden avulla. Tietotilinpäätöksessä voidaan kuvata esimerkiksi seuraavat asiat:

- mitä henkilötietoja yrityksellä on hallussa ja missä
- tiedoista vastuussa olevan henkilön nimi sekä yhteystiedot
- kuinka opinnäytetyön alussa mainitut tietosuojaperiaatteet toteutuvat
- kyseisten henkilötietojen käsittelyn oikeusperuste, eli miksi niitä käsitellään
- miten tietojenhallinnan riskit on otettu huomioon.

Samalla tulee tarkastaa, onko joukossa turhaa tietoa sekä kuinka hyvin rekisteröidyn oikeudet toteutuvat. Tietotilinpäätöksen avulla on helpompi alkaa tarkastelemaan muutosta

vaativia kohtia ja se tukee osoitusvelvollisuutta sekä läpinäkyvyysajattelua. (Laadi tietotilinpäätös 2012, 3.)

Kun tietotilinpäätös on tehty ja korjausta vaativat kohdat on havaittu, voi sen muokata ajan tasalla olevaksi selosteeksi, yhdeksi tietosuojavastaavan työkaluksi. Seloste muistuttaa laajempaa versiota rekisteriselosteesta.

Selosteet on pyydettäessä saatettava valvontaviranomaisen saataville (EU yleinen tietosuojalaki artikla 30 kohta 4).

5.3 Rekisteri- ja tietosuojaseloste

Henkilötietolain 10§:n mukaan rekisterinpitäjän tulee laatia henkilötietorekistereistä seloste, josta ilmenee tietojen käsittelyn perusteet. Rekisteriselosteessa tulee olla näkyvillä seuraavat tiedot:

- rekisterinpitäjän nimi sekä yhteystiedot
- käsittelyn tarkoitus
- kuvaus henkilötietoryhmistä
- tieto henkilötietojen mahdollisesta luovutuksesta
- kuvaus rekisterin suojauksen periaatteista EU yleisen tietosuoja-asetuksen artiklan 32 mukaan.

Rekisteriseloste on pidettävä jokaisen nähtävillä, esimerkiksi yrityksen internetsivuilla. (Henkilötietolaki 10§). Selosteen on oltava kirjallinen, sekä fyysisenä paperiversiona että sähköisessä muodossa (EU yleinen tietosuojalaki artikla 30 kohta 3).

Tietosuojaseloste on rekisteriselostetta hieman laajempi seloste. Se sisältää samat tiedot kuin rekisteriseloste, mutta lisäksi tietoa rekisteröidyn oikeuksista. (Tietosuojavaltuutetun toimisto 2018.)

5.4 Seloste käsittelytoimista

Samalla kun henkilötietolaki velvoittaa rekisteriselosteeseen, niin yleisen tietosuojalain 30 artikla velvoittaa pitämään yllä selostetta kaikista yrityksen vastuulla olevista käsittelytoimista. Selosteen tulee sisältää seuraavat tiedot:

- rekisterinpitäjän ja tietosuojavastaavan nimi ja yhteystiedot
- käsittelyn tarkoitukset
- kuvaus rekisteröityjen ryhmästä ja henkilötietoryhmistä
- henkilötietojen vastaanottajien ryhmät, joille henkilötietoja on luovutettu tai luovutetaan, mukaan lukien kolmansissa maissa tai kansainvälisissä järjestöissä
- tarvittaessa tieto henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle
- mahdollisuuksien mukaan tietoryhmien poistamisen määräajat
- mahdollisuuksien mukaan yleinen kuvaus artikla 32 1 kohdassa tarkoitetuista turvatoimista. (EU yleinen tietosuojalaki artikla 30 kohta 1.)

Edellä mainittu artikla velvoittaa myös henkilötietojen käsittelijät pitämään yllä selostetta heidän käsittelemistään tiedoista rekisterinpitäjän lukuun. Artiklan 30 2 kohdassa on kuvattu henkilötietojen käsittelijän selosteen sisältämät tiedot. Henkilötietojen käsittelijän selosteen vaatimukset ovat suppeammat, mutta ylläkuvattu seloste on suositeltava käyttää molemmissa tilanteissa. Kaikkien selosteiden on oltava aina yrityksissä ajantasaisia ja niitä on päivitettävä säännöllisin väliajoin.

5.5 Tietosuojavastaavan nimittäminen

EU:n yleinen tietosuojalaki velvoittaa rekisterinpitäjät nimittämään tietosuojavastaavan. Tietosuojavastaavan nimittäminen tuo selkeyttä ja helppoutta lain noudattamiselle. Vaikkei nimittäminen ole pakollista kaikissa tapauksissa, se on kuitenkin monin tavoin suositeltavaa. Tietosuojavastaavaa voisi kutsua yrityksen tietosuojan eräänlaiseksi peruspilariksi.

Tietosuojalain mukaan konserni voi nimittää yhden ainoan tietosuojavastaavan. Tämä kuitenkin edellyttää sitä, että kyseinen tietosuojavastaava on helposti tavoitettavissa kaikista konsernin toimipaikoista. Tietosuojavastaavan nimi ja yhteystiedot tulee julkaista ja ilmoittaa valvontaviranomaiselle. (EU yleinen tietosuojalaki artikla 37 kohdat 2 & 7.) Tietosuojavastaavan yhteystiedot ilmoitetaan valvontaviranomaiselle 25.5.2018 Tietosuojavaltuutetun toimiston internetsivulla aukeavan ilmoituslomakkeen avulla.

Käytännössä tietosuojavastaava pitää rekisteriä käsittelytoimista niiden tietojen perusteella, joita henkilötietojen käsittelystä vastaavat organisaation eri osastot hänelle toimittavat (Tietosuojavastaavia koskevat ohjeet 2017, 21). Kohdeyrityksessä tämä voisi tarkoittaa sitä, että tietosuojavastaava ylläpitää aikaisemmin mainittua tietotilinpäätöstä. Tietotilinpäätöksestä puolestaan tulee ilmi eri henkilötietoryhmät yrityksessä ja niistä vastuussa oleva henkilö.

Työnantajan on tuettava tietosuojavastaavaa hänen tehtävissään sekä varata tarpeeksi resursseja tämän tehtävien suorittamiseen. Tietosuojavastaavan tulee raportoida rekisterinpitäjän ylimmälle johdolle, eli kohdeyrityksen tapauksessa konsernin toimitusjohtajalle. (Tietosuojavastaavaa koskevat ohjeet 2017, 16.)

Yrityksen työntekijät eli rekisteröidyt ottavat yhteyttä tietosuojavastaavaan kaikissa heidän henkilötietojaan koskevissa käsittelyissä ja heidän oikeuksiensa toteuttamisessa. Tietosuojavastaava on salassapitovelvollinen suorittaessaan tehtäviään. (EU yleinen tietosuojalaki artikla 38 kohdat 4 & 5.)

5.6 Tietosuojavastaavan tehtävät

Yleinen tietosuojalaki velvoittaa tietosuojavastaavalle seuraavat tehtävät (artikla 39):

- ohjeistaa ja neuvoa rekisterinpitäjää sekä henkilötietoja käsitteleviä työntekijöitä asioissa, jotka koskevat asetuksen noudattamista
- valvoa asetuksen noudattamista konsernissa
- tehdä yhteistyötä valvontaviranomaisen kanssa sekä toimia yhteyshenkilönä valvontaviranomaiselle
- valvoa tietosuojaa koskevan vaikutustenarvioinnin toteutumista.

Tietosuojavastaavan ydintehtävän voisi tiivistää henkilötietojen käsittelyn keskushenkilöksi niin, että hän tietää aina missä mitäkin tapahtuu. Näin se on selkeää mahdollisen valvontaviranomaisen yhteydenoton tullen, kun yksi henkilö yrityksessä osaa antaa kaikki tiedot sekä osoittaa ja kertoa tarvittavat kohdat henkilötietojenkäsittelystä. Tietosuojavastaavan nimittäminen tuo selkeyttä sekä toimivuutta henkilötietojen käsittelyyn.

5.7 Ilmoitusvelvollisuus

Rekisterinpitäjällä on aina ilmoitusvelvollisuus. Tietoturvaloukkauksen sattuessa, rekisterinpitäjän on viipymättä ilmoitettava siitä valvontaviranomaiselle. Ilmoittamisen aikaraja on 72 tuntia. Mikäli ilmoitusta ei tehdä aikarajan puitteissa, rekisterinpitäjältä vaaditaan siihen pätevä selitys. Lisäksi rekisterinpitäjän on dokumentoitava kaikki tapahtuvat tietoturvarikkomukset valvontaviranomaista varten. (Tietosuojavaltuutetun toimisto 2018; EU yleinen tietosuojalaki artikla 33 kohta 1.)

Tietoturvaloukkauksen ilmoituksen voi jättää tekemättä ainoastaan silloin, jos loukkauksesta ei todennäköisesti aiheudu rekisteröidyn oikeuksiin/vapauksiin kohdistuvaa riskiä. Rekisteröidylle itselleen ilmoitus on puolestaan tehtävä joka tapauksessa ilman aiheetonta viivästystä. (Talus ym. 2017, 32.)

5.8 Rekisteröidyn oikeuksien noudattaminen

Rekisterinpitäjä on velvollinen noudattamaan kaikkia rekisteröidyn oikeuksia kuten esimerkiksi unohdetuksi tulemisen oikeutta sekä tietojen oikaisua koskevaa oikeutta. Rekisteröidyn oikeudet kuvataan tarkemmin opinnäytetyön seuraavissa vaiheissa.

6 Tietojenkäsittelyn turvallisuus ja tietoturva

Nykyään melkein kaiken tiedon ollessa digitaalisessa muodossa, on erityisen tärkeää kiinnittää huomiota käsittelyn turvallisuuteen. Yrityksen tulee varmistaa, että kaikin eri tavoin säilytettäviä tietoja säilytetään oikein. Käsittelyn turvallisuudesta puhuttaessa on otettava huomioon uusin tekniikka, käsittelyn luonne, asiayhteys sekä rekisteröidyn oikeuksien rikkomiseen liittyvät riskit.

Rekisterinpitäjän vastuulla on ottaa huomioon nämä yllä mainitut seikat ja varmistaa asianmukaiset tekniset sekä organisatoriset toimenpiteet riskiä vastaavan turvallisuustason varmistamiseksi. Tällaisia toimenpiteitä ovat esimerkiksi:

- kyky taata järjestelmien luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus
- kyky palauttaa nopeasti tietojen saatavuus ja nopea pääsy henkilötietoihin fyysisen tai teknisen vian sattuessa
- menettely, jolla testataan ja arvioidaan teknisten organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi
- henkilötietojen pseudonymisointi, jota voi käyttää arkaluontoisten, esimerkiksi terveyteen liittyvien, tietojen käsittelyyn. (EU yleinen tietosuojalaki artikla 32 kohta 1.)

Teknisillä toimenpiteillä tarkoitetaan tietoturvaa sekä teknisiä suojaustoimenpiteitä uusin teknologia ja kustannukset huomioiden. Organisatorisilla toimenpiteillä puolestaan tarkoitetaan yrityksen hallinnollista tietosuojaa esimerkiksi tietosuojapolitiikkaa ja käytäntöjä, tietosuojaohjeita ja toimintamalleja sekä sertifikaatteja. (Reittu 2017, 5.)

6.1 Digitaalinen tieto

Tietoturvasta puhuttaessa toimiston arjessa, lähtökohtana voisi olla, että jokainen työntekijä lukitsee tietokoneensa poistuessaan paikaltaan esimerkiksi ruokatunnille. Myös kirjautumisen salasanojen tulisi olla riittävän turvallisia, sisältäen isoja kirjaimia, merkkejä sekä numeroita.

Yrityksen tulee ottaa huomioon tietosuojalaki myös sisäisessä viestinnässä työpaikalla. Työpaikalla käytetään sähköpostia sekä sisäistä viestintäkanavaa. Tietosuojalain myötä esimerkiksi päämiehen lukuun käsiteltäviä henkilötietoja ei enää saakaan samalla tavalla jakaa esimerkiksi sähköpostissa.

Lisäksi esimerkiksi työsähköpostiin kirjautumista työntekijöiden henkilökohtaisilla laitteilla tulisi rajoittaa, sillä se sisältää tietoja, jotka voivat pahimmassa tapauksessa levitä ja aiheuttaa tietoturvarikkomuksia.

Uusi tietosuojalaki velvoittaa tietojen käsittelyn läpinäkyvyyteen sekä avoimuuteen, jolloin yrityksissä kannattaa jokaisen puhdistaa omat tietokoneelle tallennetut kansionsa, mikäli ne sisältävät henkilötietoja. Myös tietokoneiden tietoasemat kannattaa käydä läpi vastuualueittain.

6.2 Fyysinen tieto

Digitaalisen tiedon lisäksi melkein joka paikassa tietoa käsitellään myös fyysisessä muodossa. Fyysinen tieto, kuten mapit tulisi säilyttää lukituissa kaapeissa ja huoneissa niin ettei kaikilla ole sinne pääsyä. Pääsy tietoihin tulisi olla, kuten myös digitaalisen tiedon kohdalla, ainoastaan niillä henkilöillä, jotka työssään tarvitsevat kyseisiä tietoja.

Fyysistä tietoa säilytettäessä tulee myös selkeä tapa fyysisen tiedon tuhoamiseen sen jäädessä tarpeettomaksi. Yrityksen tulee varmistaa, ettei epämääräisiä henkilötietoja sisältäviä paperipinoja jää lojumaan toimiston pöydille tai tulostimien nurkille.

Kaiken tiedon, fyysisesti että digitaalisesti säilytettävän osalta, kannattaa yrityksen noudattaa selkeää käytäntöä, jossa tietoihin pääsee käsiksi ainoastaan ne työntekijät, joiden työtehtävien suorittaminen sitä vaatii.

7 Yritys henkilötietojen käsittelijänä

Opinnäytetyön kohdeyritys on rekisterinpitäjän roolin lisäksi myös henkilötietojen käsittelijä. Henkilötietojen käsittelijän roolia ja velvoitteita henkilötietolakiin verrattuna on kiristetty uudessa asetuksessa. Opinnäytetyön kohdeyritys käyttää ulkoisia palveluita esimerkiksi palkanmaksuyritystä, mihin kuuluu oleellisena osana myös henkilötietojen käsittely. Tässä tapauksessa ulkoistettu palvelu on henkilötietojen käsittelijä. Henkilötietojen käsittelijän on aina pystyttää osoittamaan rekisterinpitäjälle, että käsittely on asetuksen vaatimusten mukaista. Yrityksen tulee pitää yllä selostetta kaikista rekisterinpitäjien lukuun käsiteltävistä henkilötietorekistereistä. Selosteen vaatimat kohdat on kuvattu opinnäytetyön luvussa 5, Seloste käsittelytoimista.

7.1 Kokous- ja kongressiosasto

Kohdeyrityksessä toimii omana osastonaan kokous- & kongressitoimisto. He toimivat sekä rekisterinpitäjänä, että henkilötietojen käsittelijänä. Henkilötietorekisteri koostuu asiakkaiden yhteistiedoista ja henkilötietojen käsittelyä tapahtuu asiakkaan toimeksiannosta.

Asiakasrekisterin lainmukaisuus täyttyy työn luonteen vuoksi. Tapahtumanjärjestäjällä on luonnollisesti hallussaan asiakkaiden sekä yhteistyökumppaneiden yhteystietoja. Virheettömyysvaatimuksen mukaan yhteystietojen tulee olla ajantasaisia ja niitä tulee päivittää säännöllisin väliajoin. Epätäydellisiä tai vanhentuneita henkilötietoja ei saa käsitellä. (Henkilötietolaki 2:9§.)

Asiakkaan toimesta tapahtuvaa henkilötietojen käsittelyä tapahtuu esimerkiksi tapahtumien ilmoittautumis- sekä majoitusjärjestelyitä tehtäessä.

7.2 Rekisteriseloste

Henkilötiedon käsittelijän ylläpitämä rekisteriseloste poikkeaa hieman aikaisemmin tässä työssä kuvatusta rekisterinpitäjän rekisteriselosteesta. Selosteen tulisi sisältää seuraavat tiedot (EU yleinen tietosuojalaki artikla 30 kohta 2):

- henkilötietojen käsittelijän sekä rekisterinpitäjän nimi ja yhteystiedot

- kunkin rekisterinpitäjän lukuun suorittamat käsittelyiden ryhmät
- tarvittaessa tiedot henkilötietojen siirrosta muihin maihin
- mahdollisuuksien mukaan yleinen kuvaus artikla 32 1 kohdassa kuvatuista turvatoimista.

Henkilötietojen käsittelijä ei saa käyttää toisen henkilötietojen käsittelijän palveluita ilman rekisterinpitäjän erillistä lupaa. Henkilötietojen käsittelijän täytyy käsitellä tietoja ainoastaan rekisterinpitäjän antamien ohjeiden mukaisesti ja varmistaa että kaikki henkilötietoja käsittelevät henkilöt ovat salassapitovelvollisia. (EU yleinen tietosuojalaki artikla 28 kohta 2.)

Tapahtumissa kokous- ja kongressiosasto käyttää erilaisia ilmoittautumislomakkeita, jotka sisältävät tietoja osallistujasta. Tapahtumien ilmoittautumislomakkeissa ja niitä käsiteltäessä, henkilötietojen käsittelyyn on kiinnitettävä erityistä huomiota. Ilmoittautumisia tulostetaan sekä mapitetaan, jotta esimerkiksi laskutus sujuisi kätevimmin. Ilmoittautumisia tulostaessa olisi varminta käyttää tulostinta toimistohuoneessa tai esimerkiksi turvatulostusta, mikäli tulostin sijaitsee kauempana. Näin varmistettaisiin tietojen turvallisuus.

7.3 Henkilötietojen käsittely päämiehen lukuun

Kohdeyritys käsittelee henkilötietoja päämiehen lukuun. Päämies on antanut omat ohjeistuksensa yrityksen työntekijöille, kuinka heidän tulee jatkossa toimia eri tavalla henkilötietoja käsitellessään. Esimerkkinä e-learning kurssi, joka kaikkien päämiehen lukuun töitä tekevän tulee suorittaa. Lisää ohjeistuksia päämieheltä on odotettavissa loppukevään ajan.

Lisäksi myös yrityksen henkilötietojen käsittelijät ovat ilmoittaneet uusista käytänteistä, joita yleinen tietosuojalaki tuo tullessaan ja kuinka ne vaikuttavat kohdeyrityksen toimintaan, esimerkiksi sähköpostin suojaustoiminto arkaluonteisten tietojen lähetykseen.

8 Sopimukset

Tämä sopimusosuus koskee yritystä rekisterinpitäjänä, että henkilötietojen käsittelijänä. Lain vaatimia muutoksia tehdessä on hyvä tarkastaa jo voimassa olevat, ulkoistettujen palveluiden tuottajien kanssa tehdyt sopimukset. Tietosuojalaki velvoittaa, että henkilötietojen käsittelijän suorittamaa tietojenkäsittelyä rekisterinpitäjän lukuun on määritettävä sopimuksella. Tässä sopimuksessa tulee käydä ilmi muun muassa seuraavat asiat (EU yleinen tietosuojalaki artikla 28 kohta 3):

- henkilötietojen käsittelyn kohde ja kesto
- käsittelyn luonne ja tarkoitus
- henkilötietojen tyyppi ja rekisteröityjen ryhmät
- rekisterinpitäjän velvollisuudet ja oikeudet.

Mikäli edellä mainitut asiat puuttuvat, on ne helppo lisätä päivittämällä sopimukset tietosuoja-asetuksen vaatimuksia vastaaviksi. Lisäksi sopimuksessa on säädettävä, että ulkoistettu henkilötietojen käsittelijä käsittelee tietoja ainoastaan rekisterinpitäjän antamien ohjeiden mukaisesti. Lisäksi tulee varmistaa, että henkilötietoja käsittelevä yritys toteuttaa kaikki tietosuojalain 32 artiklan, käsittelyn turvallisuus, vaatimat toimenpiteet. (EU yleinen tietosuojalaki artikla 28.)

9 Rekisteröidyn oikeudet

Voimaan astuvan tietosuojalain yksi merkittävämpiä tavoitteita on turvata henkilötietojen suojaa perusoikeutena ja rekisterinpitäjän velvollisuus on noudattaa näitä oikeuksia. Kaikissa tietosuoja-asetuksen vaatimissa toimenpiteissä rekisterinpitäjän tulee pyrkiä avoimeen ja läpinäkyvään toimintaan sekä viestintään käsittelytoimista. Rekisteröidyn oikeudet tulee saattaa työntekijöiden tietoisuuteen, mikä lisää luotettavuutta yrityksen sisällä.

9.1 Pääsy omiin tietoihin

Rekisteröidyllä on oikeus saada pääsy omiin henkilötietoihinsa, eli hänellä on milloin tahansa oikeus pyytää tietonsa nähtäväksi. Tällöin rekisterinpitäjän on toimitettava kopio käsiteltävistä tiedoista rekisteröidylle. Lisäksi on ilmoitettava seuraavat kohdat:

- miksi tietoja käsitellään
- käsiteltävät henkilötietoryhmät
- tietojen luovutus kolmansille osapuolille ja tieto siitä kenelle luovutetaan
- tietojen säilytysaika
- kaikki rekisteröidyn oikeudet sekä oikeus tehdä valitus valvontaviranomaiselle.

Tietojen kerääminen voi viedä aikaa, mikäli ne eivät ole helposti saatavilla. Yrityksen tulisi siis varmistaa oikeanlainen tietojen käsittely ja että tällaisen vaatimuksen tullessa tietojen koonti on helppoa ja vastausaika rekisteröidylle mahdollisimman lyhyt. (EU-tietosuojan kokonaisuudistus 2018, 14-15.)

9.2 Oikeus tulla unohdetuksi

Tietosuoja-asetuksen mukaisesti rekisteröidyllä on oikeus vaatia tietojaan poistettavan henkilötietorekisteristä, esimerkiksi virheelliset tai vanhentuneet henkilötiedot. Rekisteröidyllä on oikeus peruuttaa sopimus henkilötietojen käsittelystä. Sopimuksen perumisen kuuluisi olla yhtä helppoa kuin sopimuksen syntymisen. (EU-tietosuojan kokonaisuudistus

2018, 15-16.) Henkilötietojen poisto rekisteristä tulee tapahtua ilman aiheettomia viivästyksiä lukuun ottamatta tilannetta, jossa tietojen säilytykselle on olemassa laillinen peruste.

Henkilötietojen poisto rekisteristä vaatii aina jonkin seuraavista perusteista:

- rekisteröity peruuttaa suostumuksensa, eikä käsittelyyn löydy lainmukaista perustetta
- tietoja on käsitelty lainvastaisesti
- henkilötietoja ei tarvita enää niihin tarkoituksiin, kuin tiedot on kerätty
- henkilötiedot on poistettava unionin oikeuteen tai jäsenvaltion lainsäädäntöön perustuvan rekisterinpitäjään sovellettavan lakisääteisen velvoitteen noudattamiseksi. (EU yleinen tietosuojalaki artikla 17 kohta 1.)

9.3 Vastustamisoikeus

Asetuksen myötä rekisteröidyllä on oikeus vastustaa henkilötietojensa käsittelyä. Vastustamisoikeutta käytettäessä, rekisterinpitäjä ei enää saa käsitellä kyseisen henkilön tietoja. Tämän avulla yksityisen henkilön on tulevaisuudessa helpompaa kieltäytyä esimerkiksi suoramarkkinoinnista. (EU yleinen tietosuojalaki artikla 17.)

Lisäksi rekisteröity voi viedä asian tietosuojavaltuutetun käsiteltäväksi, mikäli hän katsoo tai epäilee, ettei henkilötietojen käsittely ole hänen tietojensa kohdalla lainmukaista (HE 9/2018, Tietosuojalaki 4:21§).

Tässä opinnäytetyössä käsiteltiin niitä rekisteröidyn oikeuksia, jotka koskettavat kohdeyrityksen toimintaa sekä henkilötietojen käsittelyä.

10 Sanktiot ja valvontaviranomainen

Merkittävänä muutoksena tietosuojalaki tuo rangaistukset asetuksen velvoitteiden rikkomiselle. Tuntuva sakko voi enimmillään olla 20 miljoonaa euroa tai 4% yrityksen edeltävän tilikauden liikevaihdosta. Sanktion määrää valvontaviranomainen ja sen suuruus riippuu laiminlyönnin luonteesta. Samat sanktiot koskevat sekä rekisterinpitäjiä että henkilötietojen käsittelijöitä. (EU-tietosuojan kokonaisuudistus, 6-7.)

Ennen rahallista sanktiota Suomessa on mahdollista saada joissain tapauksissa myös esimerkiksi varoitus tai huomautus ennen kovempien sanktioiden käyttöönottoa. Sanktioita määrätessä, on mahdollista, että jäsenvaltioiden oma henkilötietolainsäädäntö määrää toimintaa taustalla.

Lisäksi rekisterinpitäjä on velvollinen korvaamaan rekisteröidylle vahingot, jotka ovat aiheutuneet lain vastaisesta henkilötietojen käsittelystä (Henkilötietolaki 10:47§).

Tietosuoja-asetuksessa tarkoitettuna valvontaviranomaisena Suomessa toimii tietosuojavaltuutettu. Tietosuojavaltuutettu on toiminnassaan itsenäinen ja riippumaton ja se toimii oikeusministeriön yhteydessä. (HE 9/2018, Yksityiskohtaiset perustelut 3 luku.) Valvontaviranomaiselle on määrätty erilaisia tutkintavaltuuksia sekä toimivaltuuksia. Nämä valtuudet sekä muut valvontaviranomaisen tehtävät ovat säädetty EU:n yleisen tietosuojalain artiklassa 58. Suomessa tietosuojavaltuutetun tehtävät ja toimivaltuudet tulevat suoraan EU:n yleisestä tietosuojalaista (HE 9/2018, Yksityiskohtaiset perustelut 3 luku).

Hallitus on luonut esityksen (HE 9/2018) eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi. Esityksessä ehdotetaan säädettäväksi tietosuojalaki. Lain olisi määrä korvata muun muassa henkilötietolaki ja sen tarkoitus olisi olla yleislaki kaikkien henkilötietojen käsittelyyn. Ehdotettu tietosuojalaki koostuu yleistä tietosuoja-asetusta tukevista kohdista ja sitä tulisikin tulkita rinnakkain GDPR:n kanssa. (HE 9/2018 Esityksen pääasiallinen sisältö.) Laki tuli voimaan 25. toukokuuta 2018.

11 Toimenpiteet yrityksessä

Opinnäytetyön aikana selvitettiin asiat, joissa yrityksellä on korjaamista ja mitä uutta tulisi tehdä, jotta lain vaatimuksiin vastattaisiin.

	Seloste käsittelytoimista	Sopimukset	Rekisteri-seloste	Rekisteröidyn oikeudet
Muu yritys	Koottu yhteen	Päivitetty tarpeen mukaan	Seloste käsittelytoimista	Koottu työntekijöiden saataville
Kokous- ja kongressi-osasto	Tehty	Päivitetty liitteillä	Tehty näkyväksi	Otettu huomioon

Taulukko 1. Toimenpiteiden kuvaus

Kohdeyrityksessä otettiin ensimmäiseksi asiaksi kartoittaa nykytilanne. Sitä alettiin tekemään kokoamalla kahteen tiedostoon selosteet käsittelytoimista. Näin ollen toteutuu yleisen tietosuojalain 30 artiklan vaatima selostevaatimus. Selosteet tehtiin kaikista rekisterinpitäjän vastuulla olevista käsittelytoimista, johon kuuluu esimerkiksi kaikki oman henkilökunnan tiedot. Lisäksi tehtiin toinen seloste kaikista käsittelytoimista, joita yritys tekee rekisterinpitäjien lukuun. Selosteita tullaan päivittämään aktiivisesti.

Toisena asiana otettiin selvää sopimuksista, joihin tulisi tehdä muutoksia ja joihin sisältyy henkilötietojen käsittelyä yrityksen näkökulmasta sekä rekisterinpitäjän että henkilötietojen käsittelijän roolissa. Sopimuksien päivitys toteutettiin tarpeen mukaan sopimusliitteillä. Sopimusliitteet ovat tietosuojalain vaatimuksien mukaiset.

Kokous- ja kongressiosastolle tehtiin uuden pohjan mukainen rekisteriseloste, joka tulee näkyviin myös yrityksen internetsivulle. Muulle yritykselle selosteena toimii laajempi seloste käsittelytoimista. Lisäksi kongressiosastolla läpikäytiin olemassa olevat henkilörekisterit sekä niiden säilytyksen tarve kartoitettiin. Vanhoja yhteystietoja hävitettiin ja nykyisiä päivitettiin. Nyt rekisterit ovat ajan tasalla ja niitäkin päivitetään tarpeen vaatien tulevaisuudessa. Kun asiakasrekisterit ovat ajantasaisia ja ollaan tietoisia siitä, mitä tietoja säilytetään, on niistä saatava hyötykin suurempi. Tietosuoja-asetus antoi hyvän mahdollisuuden aloittaa puhtaalta pöydältä.

Lisäksi yritykseen nimitettiin tietosuojavastaava. Tietosuojavastaavan yhteystiedot ilmoitettiin tietosuojaviranomaiselle 25.5.2018 tietosuojavaltuutetun internetsivulla aukeavalla

lomakkeella. Suureen yritykseen nimitettiin yksi tietosuojavastaava niillä perustein, että hän on tavoitettavissa ja että hänen työaikansa riittää tekemään vaaditut tehtävät.

Rekisteröidyn oikeudet on nyt otettu huomioon entistä paremmin ja niistä koottiin erillinen seloste, joka saatettiin yrityksen työntekijöiden nähtäväksi. GDPR:n tullessa pakottavaksi työntekijöidenkin tietoisuus omista oikeuksistaan varmasti herää, jolloin yritys osaa vastata pyyntöihin vaaditulla tavalla.

Yritys on vastaanottanut kevään aikana ohjeita GDPR:n soveltamisesta päämiehen lukuun käsiteltävien henkilötietojen käsittelyssä. Kyseiset muutokset vaikuttavat työntekijöiden jokapäiväiseen työskentelyyn ja niitä on alettu ottaa käyttöön sitä mukaan, kun ohje uudesta toimintavasta on saatu. Ohjeistukset ovat liittyneet isona osana muun muassa sisäiseen viestintään.

12 Pohdinta

EU yleistä tietosuojalakia alettiin soveltaa 25.5.2018. Silti moni yritys vielä tekee töitä asetuksen soveltamisen eteen. GDPR tuo yrityksille paljon uusia velvoitteita ja vastuuta. Sen lisäksi se antaa yrityksille arvokkaan kilpailuedun. Mikäli yrityksellä on tietosuoja-asiat kunnossa ja se pystytään mutkattomasti osoittamaan, se antaa itsestään luotettavan kuvan esimerkiksi työntekijöilleen.

GDPR on aiheuttanut yrityksissä sekä yksityishenkilöissä paljon kysymyksiä viime aikoina. Suomessa on pitkään ollut voimassa hyvät tietosuojalait sekä yksityiselämässä että työelämän puolella. Paljon GDPR:n painottamia asioita on ollut laissa määrättynä jo tähänkin saakka.

Se, kuinka paljon työtä sekä selvitystä GDPR on yrityksissä aiheuttanut, on varmasti tullut monelle yllätyksenä. Tämä opinnäytetyö keskittyikin kuvaamaan perusasiat, jotka tulee olla kunnossa lain soveltamisesta lähtien. Kuten sanottua, osa yleisen tietosuojalain vaatimista kohdista on ollut laissa määrättynä jo ennen GDPR:n soveltamista, mutta nyt niihin varmasti kiinnitetään taas uudella tavalla huomiota.

Opinnäytetyön avulla kohdeyritykseen luotiin pohjaa uudelle tavalle käsitellä henkilötietoja. Opinnäytetyöprojektin jälkeen kehitystyö yrityksessä jatkuu edelleen ja tulevaisuudessa monikin asia saatetaan tulla tekemään toisin, mikäli niille löydetään käytännönläheisempiä toteutustapoja.

Henkilötietojen käsittelyn tärkeys korostuu tulevaisuudessa vielä enemmän mitä se nyt on. Digitalisaatio kehittyy jatkuvasti ja voidaankin pohtia, kuinka pitkälle tietojenkäsittelyn turvallisuutta voidaan tulevaisuudessa kehittää, että se tulisi aina olemaan turvallista ja väärinkäytöltä suojattua.

Lähteet

Ahola, M., & Hirvelä, U. (2016). Henkilötiedon elinkaari ja tietosuoja yritystoiminnassa. https://uutishuone.pwc.fi/henkilotiedon-elinkaari-ja-tietosuoja-yritystoiminnassa/ Luettu 11.2.2018

EU yleinen tietosuoja-asetus (2016). http://www.privacy-regulation.eu/fi/index.htm Luettu 5.1.2018.

Hallituksen esitys eduskunnalle EU:N yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi. (2018). https://www.finlex.fi/fi/esitykset/he/2018/20180009#idp451253632 Luettu 1.6.2018

Henkilötietolaki (1999). https://www.finlex.fi/fi/laki/ajantasa/1999/19990523?search%5Btype%5D=pika&search%5Bpika%5D=henkil%C3%B6tietolaki Luettu 6.2.2018

IPRA Technologies Oy. (2017). EU GDPR and email https://eezykeyz.eu/wp-content/uploads/2017/10/EU-GDPR-Email.pdf Luettu 4.4.2018

Karhula Päivikki, & Kipinoinen Kaisa. (2018). EU:N tietosuojauudistus ja sen kansallinen täytäntöönpano. https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/LATI/Sivut/EUn-tietosuojauudistus.aspx Luettu 22.3.2018

Laadi tietotilinpäätös. (2012). http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfpzNVCh/Laadi_tietotilinpaatos.pdf Luettu 18.3.2018

Laki yksityisyyden suojasta työelämässä (2004). https://www.finlex.fi/fi/laki/ajantasa/2004/20040759#L2 Luettu 1.4.2018

OpiTietosuojaa.fi. EU:N tietosuoja-asetuksen velvoitteet johdolle. https://opitietosuojaa.fi/index.php/fi/56-lainsaeaedaentoe/lait/eun-tietosuoja-asetus/23-tuleva-eu-n-tietosuoja-asetus Luettu 19.2.2018

Reittu, J. (2017). Kuinka valmistautua yleiseen tietosuoja-asetukseen? http://www.doria.fi/bitstream/handle/10024/144142/Jarkko_Reittu_Kuinka%20valmistautua%20tietosuoja-asetukseen.pdf?sequence=1 Luettu 15.4.2018

Talus, A., Autio, E., Hänninen, A., Pihamaa, H., & Kantonen, S. (2017). *Miten valmistautua EU:N tietosuoja-asetukseen?* Oikeusministeriö. http://urn.fi/URN:ISBN:978-952-259-558-4 Luettu 19.2.2018

Tietosuojavaltuutetun toimisto. (2013). Tietosuojavaltuutetun toimisto. http://www.tietosuoja.fi/fi/index/tietosuojavaltuutetuntoimisto/tehtavat.html Luettu 7.2.2018

Tietosuojavaltuutetun toimisto. (2018a). Tietosuojavaltuutetun toimisto. http://www.tietosuoja.fi/fi/index/ajankohtaista/tiedotteet/on/02/ilmoitusvelvollisuustietosuojavaltuutetuntoimistollemuuttuu25.toukokuuta.html Luettu 8.2.2018

Tietosuojavaltuutetun toimisto. (2018b). Tietosuojavaltuutetun toimisto. http://www.tietosuoja.fi/fi/index/materiaalia/lomakkeet.html Luettu 8.2.2018

Tietosuojavaltuutetun toimisto. (2018c). Tietosuojavaltuutetun toimisto. http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html Luettu 15.3.2018

Tietosuojavastaavia koskevat ohjeet (2017). Tietosuojatyöryhmä. http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/UvreCmOiN/Tietosuojavastaavia_koskevat_ohjeet_wp243rev01_fi.pdf Luettu 6.3.2018

Työsopimuslaki (2001). https://www.finlex.fi/fi/laki/ajantasa/2001/20010055#L6P7 Luettu 7.3.2018

Valtiovarainministeriö. (2016). *EU-tietosuojan kokonaisuudistus.* https://www.vah-tiohje.fi/c/document_library/get_file?uuid=c97ee414-1fc0-4a91-969c-2ef0657605d1&groupId=10128 Luettu 5.4.2018

Ylipartanen, A., & Andreasson Ari. (2017). EU:N yleinen tietosuoja-asetus (GDPR) muuttaa kansalliset käytännöt. https://opitietosuojaa.fi/index.php/fi/oikeus/lait/eu-n-tietosuoja-asetus Luettu 6.3.2018